Amendments to the claims:

1. (currently amended): An identification document comprising a photographic representation of a bearer of the identification document and indicia provided on the document, the identification document further comprising a security feature printed on a surface of the identification document in a two-dimensional encoded symbology, the security feature including:

a first set of information contained in the encoded symbology corresponding to at least one of the identification document, the bearer of the identification document or an issuer of the identification document, wherein the first set of information comprises an unencrypted form; and

a cryptographic measure contained in the encoded symbology associated with the first set of information, the cryptographic measure identifying at least a record of fabrication for the identification document.

2. (previously presented): The identification document of claim 1, wherein the record of fabrication identifies at least one of equipment used in fabricating the identification document, an identification document assembler, a distribution channel or an operator of document fabrication equipment.

3. (previously presented): The identification document of claim 1, wherein the first set of information comprises at least one of a document identifier, issuer identification, issue date, bearer's date of birth, characteristics associated with the bearer's physical attributes, bearer's name, address, document inventory number or bearer's age.

4. (previously presented): The identification document of claim 1, wherein the two-dimensional symbology comprises at least one of a 2D-barcode, data glyph, maxicode, PDF 417, DataMatrix, or QR Code.

5. (original): The identification document of claim 1, wherein the cryptographic measure comprises an encrypted form corresponding to a private key, said cryptographic measure further comprising at least one of a public key associated with the private key and information identifying where a public key associated with the private key can be obtained, wherein the private key is uniquely associated with an element of the record of fabrication.

6. (original): The identification document of claim 1, wherein said cryptographic measure comprises a cryptographic certificate.

7. (original): The identification document of claim 6, wherein the certificate comprises a public key for decrypting at least a portion of the cryptographic measure.

8. (original): The identification document of claim 6, wherein the cryptographic measure comprises an encrypted form corresponding to at least a first private key and second private key, wherein the first private key is uniquely associated with a fabrication equipment operator, and the second private key is uniquely associated with equipment used in fabricating the identification document.

9. (original): The identification document of claim 6, wherein the cryptographic measure comprises at least a first digital signature and a second digital signature, wherein the first digital signature corresponds to a first stage of a document fabrication process, and the second digital signature corresponds to a second stage of the document fabrication process.

10. (original): The identification document of claim 6, wherein the cryptographic measure comprises a hash of at least the first set of information, the hash being encrypted by the private key.

11. (original): The identification document of claim 10, wherein the hash further represents a second set of information, wherein the second set of information is supplemental to the first set of information.

12. (original): The identification document of claim 11, wherein the second set of information comprises a condensed representation of the photographic representation.

13. (original): The identification document of claim 11, wherein the second set of information comprises a document inventory number, the inventory number being conveyed by a machine-readable code carried by the identification document.

14. (previously presented): The identification document of claim 1, wherein the indicia comprises at least one of artwork, text, barcodes, graphics or digital watermarking.

15. (currently amended): A method of analyzing an identification document, the identification document comprising a security feature printed or engraved on a surface of the identification document in a two-dimensional encoded symbology, the identification document further comprising a first set of information and a cryptographic signature corresponding to the first set of information, both being contained in the encoded symbology, wherein the first set of information and the cryptographic signature are encoded in a machine-readable format, ~~the encoding being printed or engraved on a surface of the identification document~~, said method comprising:

machine-sensing the first set of information and the cryptographic signature; and

determining construction materials, equipment or processing details of the identification document from at least the cryptographic signature.

16. (original): The method of claim 15, wherein the machine-readable format comprises digital watermarking.

17. Cancelled.

18. (original): The method of claim 15, further comprising determining whether the identification document is deemed suspect based at least on the cryptographic signature.

19. (original) The method of claim 18, wherein the identification document further comprises a certificate corresponding to the cryptographic signature, and wherein the certificate

is encoded in the machine-readable format and printed or engraved on the surface of the identification document.

20. (original): The method of claim 19, wherein said determining comprises determining whether the certificate has been revoked.

21. (currently amended): A method of analyzing an identification document, the identification document a security feature printed or engraved on a surface of the identification document in a two-dimensional encoded symbology, the identification document further comprising a first set of information, and a cryptographic signature corresponding to the first set of information both being contained in the encoded symbology, wherein the first set of information and the cryptographic signature are encoded in a machine-readable format, the encoding being printed or engraved on a surface of the identification document, said method comprising:

machine-sensing the first set of information and the cryptographic signature; and

determining fabrication details of the identification document from at least the cryptographic signature, wherein said cryptographic signature comprises a date indicator, and wherein said determining comprises determining whether the date indicator corresponds with an untrusted — but not expired — date.

22. (previously presented): The method of claim 18, wherein the cryptographic signature corresponds with a symmetrical key, and said determining comprises communicating at least the first set of information and the cryptographic signature to a remote processor, the remote processor determining whether the identification document is suspect by at least decrypting the cryptographic signature with the symmetrical key.

23. (original): The method of claim 18, wherein the cryptographic signature corresponds to a pair of asymmetrical keys.

24. (previously presented) The method of claim 18, wherein the fabrication details comprise at least one of an identification document distribution record, unauthorized issuance,

type of identification document, equipment used to fabricate the document, document assembling equipment operator, document lot number or document batch number.

25. (original): The method of claim 18, wherein the fabrication details comprise at least a type of identification document, with a unique private key corresponding to the type.

26. (original): The method of claim 15, further comprising verifying the first set of information with the cryptographic signature.

27. (Currently Amended): A method of identifying unauthorized issuance of an identification document, wherein unauthorized issuance occurs when the identification document is fabricated on authorized equipment but is issued in an unauthorized manner, the identification document comprising a security feature printed or engraved on a surface of the identification document in a two-dimensional encoded symbology, the identification document further including first data and a digital signature corresponding to at least the first data, both being contained in the encoded symbology, the digital signature further including a date indicator associated with the fabrication of the identification document, said method comprising:

machine-sensing the identification document to obtain the first data and the digital signature;

validating the digital signature in accordance with a certificate associated with the digital signature;

determining whether the certificate has been revoked, and if so revoked, determining whether the date indicator corresponds with a date associated with the certificate's revocation, and if so associated,

identifying the identification document as being issued without authority.

28. (original): The method of claim 27, wherein the identification document further includes the certificate.

29. Cancelled.

30. Cancelled.

31. Cancelled.

32. Cancelled.

33 - 41. Cancelled.

GENERAL REMARKS

Claims Status:

Claims 1 through 16, 18 through 28 are pending in this application.

Claims 1, 15, 21 and 27 have been amended by this office by this Response.

Claim 17 has been cancelled.

Claims 29 to 32 have been cancelled.

Claims 33 to 41 were previously cancelled.

REMARKS ON REJECTIONS

Reconsideration and allowance of the above claims in this application is respectively requested. No new matter has been added by the amendments made herein.

In the Office Action Mailed November 10, 2008, the Examiner rejected all the claims under 35 USC §103(a) on the basis of Chow *et al.* (US 6,292,092) (hereinafter "Chow") alone or in view of one or more secondary references, depending on the specific claim, to be discussed in detail below.